

The copyright © of this thesis belongs to its rightful author and/or other copyright owner. Copies can be accessed and downloaded for non-commercial or learning purposes without any charge and permission. The thesis cannot be reproduced or quoted as a whole without the permission from its rightful owner. No alteration or changes in format is allowed without permission from its rightful owner.



**THE APPLICATION OF MALAYSIAN CYBER SECURITY
LAWS IN REGULATING CYBER INSIDER THREATS IN
MALAYSIAN ORGANISATIONS**



AFIQAH BINTI ABDUL RAZAK

**MASTER OF LAW
UNIVERSITI UTARA MALAYSIA
2025**

**THE APPLICATION OF MALAYSIAN CYBER SECURITY
LAWS IN REGULATING CYBER INSIDER THREATS IN
MALAYSIAN ORGANISATIONS**



AFIQAH BINTI ABDUL RAZAK (828932)

**A thesis submitted to the Ghazalie Shafie Graduate School of Government in
fulfilment of the requirement for the Master of Law
Universiti Utara Malaysia**



Kolej Undang-Undang, Kerajaan dan Pengajian Antarabangsa
(College of Law, Government and International Studies)
UNIVERSITI UTARA MALAYSIA

PERAKUAN KERJA TESIS
(Certification of thesis)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

AFIQAH ABDUL RAZAK (828932)

calon untuk Ijazah
(candidate for the degree of)

MASTER OF LAW (BY RESEARCH)

telah mengemukakan tesis yang bertajuk:
(has presented his/her thesis of the following title):

**THE APPLICATION OF MALAYSIAN CYBERSECURITY LAWS IN REGULATING CYBER
INSIDER THREATS IN MALAYSIAN ORGANISATIONS**

seperti yang tercatat di muka surat tajuk dan kulit tesis.
(as it appears on the title page and front cover of the thesis).

Bahawa tesis tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada **17 JULAI 2024**

*That the said thesis is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on: **JULY 17, 2024***

Pengerusi Viva : **ASSOC. PROF. DR.
(Chairman for Viva) HASLINDA MOHD ANUAR**

Tandatangan
(Signature)

Pemeriksa Luar : **ASSOC. PROF. DR. SONNY
(External Examiner) ZULHUDA (IIUM)**

Tandatangan
(Signature)

Pemeriksa Dalam : **ASSOC. PROF. DR. AHMAD
(Internal Examiner) SHAMSUL ABD AZIZ**

Tandatangan
(Signature)

Tarikh : **17 JULY 2024**
Date

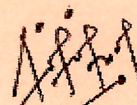
Nama Pelajar : AFIQAH ABDUL RAZAK (828932)
(Name of Student)

Tajuk Tesis : THE APPLICATION OF MALAYSIAN CYBERSECURITY LAWS IN
(Title of the Thesis) REGULATING CYBER INSIDER THREATS IN MALAYSIAN
ORGANISATIONS

Program Pengajian : MASTER OF LAW (BY RESEARCH)
(Programme of Study)

Penyelia Pertama : ASSOC. PROF. DR. ANI
(First Supervisor) MUNIRAH MOHAMAD

Tandatangan
(Signature)



PERMISSION TO USE

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Perpustakaan Sultanah Bahiyah UUM may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Ghazali Shafie Graduate School of Government (GSGSG). It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean Ghazali Shafie Graduate School of Government

UUM College of law, Government and International Studies (UUM COLGIS)



Universiti Utara Malaysia

06010 UUM Sintok

Universiti Utara Malaysia

ABSTRACT

The data security of an organisation is not only susceptible to malicious outsiders and exploitative attackers but also to insider threats. Preventing insider threats is particularly challenging, especially when they originate from seemingly trusted and authorised insiders. Currently, in Malaysia there are several legislation touch upon cyber security. Nevertheless, the regulation of cyber insider threats remain severely limited and inadequate. Organisations respond to insider threats risks by implementing their own cyber insider threat programmes. However, the extensive scrutiny and monitoring of employees that these programmes entail, may lead to dissatisfaction among employees or even a potential breach of their privacy rights. Hence, this thesis aims to study the concepts of cyber security and cyber insider threats in organisations; analyse the existing Malaysian cyber security laws related to cyber insider threats; examine the application of these laws in regulating cyber insider threats and study the strategies to balance employees' right to privacy with the potential intrusion posed by insider threats programmes. Employing a qualitative research approach, nine professionals from different backgrounds in Malaysia were interviewed using a semi-structured approach. Data was collected on the applications of existing cyber security laws in regulating cyber insider threats and cyber insider threats programmes. The study found that there is a need to revise existing cyber security provisions to better regulate cyber insider threats. In many cases, individuals involved in insider threats face legal consequences, however, there are instances where they may evade charges or receive lesser penalties. Furthermore, cyber insider threats programmes have been found to prevent incidents by implementing strategies to detect, deter, and respond to potential threats within an organisation, demonstrating their effectiveness in combating cyber threats. Nonetheless, striking a balance between the right to monitor employees against insiders' threats and the right to privacy of employees remains a critical challenge. The findings of the study are expected to contribute to the body of knowledge on cyber insider threats in Malaysia and assist the policy makers in improving the legal framework surrounding cyber insider threats and related programs.

Keywords: Cyber Security, Insider Threats, Privacy Rights, Employees' Rights, Legislation

ABSTRAK

Keselamatan data organisasi bukan sahaja tertakluk kepada ancaman luar dan penyerang eksploitasi tetapi juga kepada ancaman dalaman. Mencegah ancaman dalaman lebih mencabar kerana ia melibatkan orang dalam yang nampak dipercayai. Di Malaysia, terdapat beberapa undang-undang yang menyentuh tentang keselamatan siber. Walau bagaimanapun, liputan perundangan terhadap ancaman siber dari orang dalam ini sangat terhad dan tidak mencukupi. Organisasi telah melaksanakan program ancaman siber dari orang dalam sebagai respon mereka kepada risiko ancaman siber dari orang dalam. Walau bagaimanapun, pemeriksaan dan pemantauan yang meluas terhadap pekerja mungkin menyebabkan ketidakpuasan hati pekerja atau berpotensi melanggar hak privasi pekerja. Oleh yang demikian, tesis ini mengkaji konsep keselamatan siber dan ancaman siber dari orang dalam di dalam organisasi menganalisis undang-undang keselamatan siber sedia ada yang berkaitan dengan ancaman siber dari orang dalam di Malaysia melihat penerapan undang-undang keselamatan siber di Malaysia dalam mengawal ancaman siber dari orang dalam dan mengkaji strategi dalam mengimbangi hak privasi pekerja dan potensi pencerobohan privasi yang disebabkan oleh program ancaman siber dari orang dalam. Mengguna pakai penyelidikan kualitatif, sembilan orang profesional dari latar belakang yang berbeza dari Malaysia telah ditemubual secara separa-berstruktur. Data mengenai penerapan undang-undang keselamatan siber yang sedia ada dalam mengawal ancaman siber dari orang dalam dan program ancaman siber dari orang dalam dikumpulkan. Kajian menunjukkan bahawa terdapat keperluan untuk mengkaji semula undang-undang keselamatan siber yang sedia ada supaya dapat mengawal ancaman siber dari orang dalam dengan lebih baik. Dalam kebanyakan kes, individu yang terlibat dalam kes ancaman siber boleh dikenakan tindakan undang-undang tetapi dalam beberapa keadaan, mereka boleh melepaskan diri dari tuduhan atau dikurangkan penalti. Tambahan lagi, program ancaman siber dari orang dalam didapati dapat menghalang kes ancaman siber dengan penerapan kaedah untuk mengesan, mengelak dan bertindakbalas terhadap ancaman siber dalam organisasi. Walau bagaimanapun, keperluan kepada suatu kaedah yang mengimbangi antara hak untuk memantau pekerja terhadap ancaman orang dalam dan hak privasi pekerja kekal sebagai satu cabaran kritikal Hasil kajian ini dijangka dapat menyumbang kepada ilmu berkenaan ancaman siber dari orang dalam di Malaysia dan membantu penggubal undang-undang dalam menambah baik rangka perundangan berkaitan ancaman siber dari orang dalam dan program-program berkaitan.

Kata Kunci: Keselamatan Siber, Ancaman Siber Dari Orang Dalam, Hak Privasi, Hak Pekerja, Perundangan

ACKNOWLEDGEMENT

All praise is due to Allah, whose guidance and blessings have enabled the successful completion of this thesis. I am truly grateful for the strength, resilience, and opportunities granted to me throughout this journey.

My deepest appreciation goes to my supervisor, Associate Professor Dr. Ani Munirah Mohamad, for her invaluable guidance, patience, and insightful feedback. Her support has been fundamental to the development of this work. I also extend my gratitude to all lecturers who contributed to my academic growth along the way.

To the respondents who generously participated in this research, thank you for your time, openness, and insights. Your valuable contributions significantly enriched the quality and depth of this study.

I am also thankful to Universiti Utara Malaysia for providing essential facilities and resources, and to MARA for the support through the Graduate Excellence Program (GREP).

I owe a profound debt of gratitude to my beloved parents, Dato' Dr. Abdul Razak Saleh and Datin Siti Habsah Samad, whose constant love, prayers, and encouragement have been my greatest source of strength. To my family, thank you for your endless support and understanding, especially during challenging moments. Lastly, I wish to thank my friends and colleagues, whose kindness, encouragement, and companionship have made this journey more meaningful. Your presence has been a source of motivation, and I am truly grateful.

This thesis is a reflection of not only my efforts, but also the collective support, guidance, and kindness of many individuals. To all who have contributed in ways both seen and unseen, please accept my deepest thanks.

TABLE OF CONTENTS

PERMISSION TO USE.....	i
ABSTRACT.....	ii
ABSTRAK.....	iii
ACKNOWLEDGEMENT	iv
TABLE OF CONTENTS.....	v
LIST OF TABLES	vi
LIST OF FIGURES	vii
LIST OF STATUES	vii
LIST OF CASES.....	ix
LIST OF ABBREVIATIONS.....	x
CHAPTER ONE INTRODUCTION	1
1.1 Introduction	1
1.2 Problem Statement	3
1.2.1 The adequacy of the existing laws in governing cyber insider threats.....	5
1.2.2 Inadequate cyber insider threat management programs within organisations to combat cyber insider threats	6
1.2.3 Achieving an appropriate balance between the employees' right to privacy and the intrusion caused by cyber insider threat programmes	7
1.3 Research Questions	8
1.4 Research Objectives	9
1.5 Significance of the Study	9
1.6 Research Methodology.....	10
1.6.1 Research Design.....	11
1.6.2 Types of Data	12
1.6.3 Data Collection Methods.....	13
1.6.4 Analysis of Data	14
1.7 Scope of Study	15
1.8 Research Ethics	16
1.9 Limitations of the Study	17
1.10 Operational Definition.....	17
1.11 Literature Review	21
1.11.1 Conceptual Framework	21

1.11.2 Theoretical Framework	28
1.11.3 Legal Framework	31
1.12 Outline of Chapters	37
1.13 Conclusion.....	41
CHAPTER TWO BACKGROUND OF RESEARCH	42
2.1 Introduction.....	42
2.2 Conceptualisation of Cyber Security and Cyber Insider Threats.....	43
2.2.1 Cyber Security	44
2.2.2 Cyber Insider Threat	49
2.3 Historical Background	59
2.3.1 Cyber Insider Threat	64
2.3.2 Cyber Insider Threat Program	65
2.3.3 Employees' right to privacy versus CIT programs	67
2.4 Brief Legal Framework.....	71
2.4.1 Communications and Multimedia Act of 1998.....	71
2.4.2 Computer Crimes Act 1997	72
2.4.3 Personal Data Protection Act 2010	72
2.4.4 Cyber Security Act 2024.....	72
2.5 Institutional Framework.....	73
2.6 Conclusion	74
CHAPTER THREE THE EXISTING LAWS ON MALAYSIAN CYBER SECURITY LAW RELATING TO CYBER INSIDER THREAT MANAGEMENT	77
3.1 Introduction.....	77
3.2 Communications and Multimedia Act 1998	77
3.2.1 About CMA	77
3.2.2 CMA and regulation of cyber insider threats.....	81
3.2.3 CMA provisions in the context of cyber insider threats	85
3.2.4 Adequacy of Sections 233 and 236 in regulating cyber insider threats	85
3.3 Computer Crimes Act 1997	87
3.3.1 About CCA	87
3.3.2 CCA and regulation of cyber insider threats.....	91
3.3.3 CCA provisions in the context of cyber insider threats	93

3.3.4 Adequacy of Sections 3, 4 and 5 of CCA in regulating cyber insider threats	95
3.4 Personal Data Protection Act 2010	97
3.4.1 About PDPA	97
3.4.2 PDPA and regulation of cyber insider threat	104
3.4.3 PDPA provisions in the context of cyber insider threat.....	105
3.4.4 Adequacy of the Security Principles of PDPA in regulating cyber insider threats	108
3.5 Cyber security Act 2024.....	110
3.7 Conclusion	116

CHAPTER FOUR THE APPLICATION OF MALAYSIAN CYBER SECURITY PROVISIONS IN REGULATING CYBER INSIDER THREATS IN MALAYSIAN ORGANISATIONS..... 117

4.1 Introduction.....	117
4.2 Implications of Cyber Insider Threat Incidents	127
4.2.1 Financial Loss	127
4.2.2 Reputational Damage.....	129
4.2.3 Legal and regulatory penalties	131
4.2.4 Disruption of business operations	133
4.2.5 Loss of intellectual property	134
4.3 Incidents caused by insider threats in Malaysian Organisation	136
4.3.1 Monetary Gain or Revenge	138
4.3.2 Negligence and Carelessness	139
4.4 Prayers prayed by prosecutions.....	140
4.5 The Application of the cyber security legal provisions and the Offenders' Defence Strategy	142
4.6 Conclusion	145

CHAPTER FIVE THE BALANCING STRATEGY BETWEEN EMPLOYEES' RIGHT TO PRIVACY AND THE INTRUSION CAUSED BY CYBER INSIDER THREAT PROGRAMMES 146

5.1 Introduction.....	146
5.2 Importance and Necessity of Cyber Insider Threat Programs	146

5.3 Cyber insider threat program as a mechanism to prevent cyber insider incidents	151
5.4 The Intrusiveness of Cyber Insider Threat Program	154
5.5 Privacy Rights of Employees	158
5.6 Balancing the employees' right to privacy and the intrusion caused by cyber insider threat programmes	163
5.7 Conclusion	171
CHAPTER SIX DISCUSSION & CONCLUSION.....	173
6.1 Introduction	173
6.2 Key Findings	174
6.2.1 The concepts of cyber security and cyber insider threats in organisations	175
6.2.2 The Existing Laws on Malaysian Cyber Security Relating to the Cyber Insider Threats Management.....	176
6.2.3 The Application of Malaysian Cyber Security Laws in Regulating Cyber Insider Threats In Malaysian Organisations.....	177
6.2.4 The Balancing Strategy Between Employees' Right to Privacy and The Intrusion Caused by Insider Threat Programmes.....	179
6.3 Suggestions and Recommendations	180
6.3.1 Roles of Parliament.....	180
6.3.1.1 Communications and Multimedia Act of 1998	180
6.3.1.2 Computer Crimes Act 1997	182
6.3.1.3 Personal Data Protection Act 2010.....	183
6.3.2 Roles of Regulators & Government Agencies.....	183
6.3.2.1 Role of Malaysian Communications and Multimedia Commission (MCMC)	183
6.3.2.2 Role of Royal Malaysia Police (RMP)	185
6.3.2.3 Role of Personal Data Protection Department (PDPA).....	186
6.3.3 Roles of Organisations	187
6.3.3.1 Board of Directors	187
6.3.3.2 Legal Officers	188
6.3.3.3 IT Officers	189

6.3.3.4 Risk Management Officer (RMO).....	190
6.4 Future Research.....	190
6.5 Concluding Remarks.....	191
REFERENCES.....	194
APPENDIX.....	206



LIST OF TABLES

Table 1. Respondents of the interviews	14
Table 2. Measures to Curb Cyber Insider Threats	65
Table 3. Balancing the employees' right to privacy and the intrusion caused by cyber insider threat programmes.....	169



LIST OF FIGURES

Figure 1. Conceptual framework of the Study	50
Figure 2. Cyber Insider Threats in Organisations	137



LIST OF STATUTES

Communications and Multimedia Act of 1998

Computer Crimes Act 1997

Cyber security Act 2024

Personal Data Protection Act 2010



LIST OF CASES

<u>Case 1.</u> PP v Roslan and Anor [2016] 1 LNS 651	32
Case 2. PP v Vishnu Devarajan [2016] 1 LNS 1066	33
Case 3. Chan Ah Kien v. Brite-Tech Berhad & Anor [2019] MLJU 2017.....	33
Case 4. Schmidt Scientific Sdn Bhd v Ong Han Suan, [1997] 5 MLJ 632.....	33
Case 5. Toh See Wei v Teddric Jon Mohr & Anor [2017] 11 MLJ 67.....	34
Case 6. Nik Adib Nik Mat v PP [2017] 1 LNS 2182.....	78
Case 7. Mohd Fahmi Reza bin Mohd Zarin lwn Pendakwa Raya [2020] 7 MLJ 399	78
Case 8. Ong Eng Guan v. Public Prosecutor [1956] 1 MLJ 44	79
Case 9. Celcom (Malaysia) Bhd & Anor v. Tan Sri Dato’ Tajudin Ramli & Ors [2022] 4 CLJ 381	79
Case 10. Teoh Kah Yong v. Public Prosecutor [2022] 1 LNS 2982.....	80
Case 11. PP v Amar Asyraf Zolkepli [2021] 1 CLJ 843.....	89
Case 12. Roslan Mohamad Som & Anor v Pendakwa Raya [2016] 1 LNS 651	89
Case 13. Kangaie Agilan Jammaany v PP [2017] 1 LNS 1640.....	90
Case 14. Genting Malaysia Bhd v Pesuruhjaya Perlindungan Data Peribadi & Ors [2022] 4 CLJ 399.....	102
Case 15. Public Bank Berhad v Tan Teck Seng Jason & Anor [2021] 1 LNS 97	104
Case 16. <i>Douglas v Hello! Ltd</i> [2005] EWCA Civ 595.....	159
Case 17. Dr Bernadine Malini Martin v MPH Magazines Sdn Bhd [2010] 7 CLJ 525.....	160
Case 18. Maslinda Ishak v Mohd Tahir Osman [2009] 6 CLJ 653.....	160
Case 19. Sivarasa Rasiah v Badan Peguam Malaysia & Anor [2010] 2 MLJ 333	160
Case 20. Ultra Dimension v Kook Wei Kuan [2004] 5 CLJ 285.....	161

LIST OF ABBREVIATIONS

CCA	Computer Crimes Act 1997
PDPA	PDPA
CMA	Communication and Multimedia Act 1998
CCTV	Closed-circuit television
CSA	Cyber Security Act 2024
NCIISL	National Critical Information Infrastructure Sector Lead
NCIIE	National Critical Information Infrastructure Entity
EU	European Union
ISMS	Information Security Management System
NSA	National Security Agency
US	United States
MyCERT	Malaysian Computer Emergency Response Team
MCMC	Malaysian Communications and Multimedia Department
PDPD	Personal Data Protection Department

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The data security of an organisation is not only susceptible to malicious outsiders and exploitative attackers, but also to insider threats. An insider threat can be defined as a security danger that arises from inside the organisation itself. This risk concerns a business associate or an employee who is permitted to access the organisation's sensitive records or accounts and wrongly uses such access. The existing security measures relatively centre on outsider threats and incapable of discovering and preventing insider threat.

An insider threat is considered to be even more dangerous for it does not require a malicious intention. Preventing insider threat is difficult for the trusted and authorised insiders are involved in it¹. An insider can be interpreted in terms of two basic acts: clear breach of security policies through authorized access and clear breach of security policies through unauthorised access.² In the first scenario, the insider utilises their authorized access to perform a specific action that violates the security policy, such as when confidential material is leaked to an outsider. In this case, the insider is authorised to access the resources, but he or she utilises that authority to pass the information to someone who are not authorised to ingress them (or to disallow authorised person to access such information).

¹ Pratik Chattopadhyay , Lipo Wang , and Yap-Peng Tan, "Scenario-Based Insider Threat Detection From Cyber Activities", IEEE Transactions On Computational Social Systems, Vol. 5, No. 3, (September 2018), https://www.researchgate.net/publication/327194848_Scenario-Based_Insider_Threat_Detection_From_Cyber_Activities (accessed November 21, 2021)

² Matt Bishop and Carrie Gates, "Defining Insider Threat", (2008), https://www.researchgate.net/publication/228993616_Defining_the_Insider_Threat (accessed November 18, 2021)

References

- “A Brief History of cyber security and Hacking.” 2020. Cybernews. October 2020. <https://cybernews.com/security/brief-history-of-cyber-security-and-hacking>.
- “Cyber Security Malaysia.” n.d. Ww. cyber security.my. https://www.cybersecurity.my/en/our_services/mycert/main/detail/2328/index.html.
- “Definition of INSIDER.” Ww. merriam-Webster.com. <https://www.merriam-webster.com/dictionary/insider>.
- “Former Morgan Stanley Financial Adviser Sentenced in Manhattan Federal Court for Illegally Accessing Confidential Client Information.” 2015. Ww. justice.gov. December 22, 2015. <https://www.justice.gov/usao-sdny/pr/former-morgan-stanley-financial-adviser-sentenced-manhattan-federal-court-illegally-0>.
- “How to Build an Insider Threat Program [10-Step Checklist].” 2021. Ww. ekransystem.com. February 10, 2021. <https://www.ekransystem.com/en/blog/insider-threat-program>.
- “Insider Definition & Meaning | Britannica Dictionary.” n.d. Ww. britannica.com. <https://www.britannica.com/dictionary/insider>.
- “Malaysia: The Cyber security Bill 2024 - a New Era for Cyber security - Baker McKenzie InsightPlus.” 2024. Bakermckenzie.com. 2024. <https://insightplus.bakermckenzie.com/bm/data-technology/malaysia-the-cyber-security-bill-2024-a-new-era-for-cyber-security..>
- “Malaysia: The Cyber security Bill 2024 - a New Era for Cyber security - Baker McKenzie InsightPlus.” 2024. Bakermckenzie.com. 2024. <https://insightplus.bakermckenzie.com/bm/data-technology/malaysia-the-cyber-security-bill-2024-a-new-era-for-cyber-security>.
- “National Insider Threat Task Force (NITTF).” 2018. Dni.gov. 2018. <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf>.
- “Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience.” World Economic Forum 2012. <https://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience>.
- “Robert T. Craig and Heidi L. Muller (Eds), Theorizing Communication: Readings across Traditions. Los Angeles, London, New Delhi and Singapore: Sage,

2007. US\$44.95. 525 Pp.” 2008. *European Journal of Communication* 23, no. 2 (June): 257–58. <https://doi.org/10.1177/02673231080930020502>.
- “TM’s Addresses Data Breach of Unifi Mobile Customers Contact Information | Telekom Malaysia.” n.d. Tm.com.my. <https://tm.com.my/news/tm-addresses-data-breach-unifi-mobile-customers-contact-info>.
- “What Is an Insider Threat | Malicious Insider Attack Examples | Imperva.” n.d. Learning Center. <https://www.imperva.com/learn/application-security/insider-threats>.
- A. de Vaus, David. 2001. *Research Design in Social Research*. 2nd edn. SAGE Publications Inc .
- Abdul Aziz, Omar Saifuddin, Rinesha Samuel, Demetria and Azami, Nur Amalina “Privacy Law in Malaysia - Azmi & Associates.” 2023. Azmi & Associates. August 2, 2023. <https://www.azmilaw.com/insights/privacy-law-in-malaysia>.
- Acemyan, Claudia Ziegler, Philip Kortum, Jeffrey Xiong, and Dan S. Wallach. 2018. “2FA Might Be Secure, but It’s Not Usable: A Summative Usability Assessment of Google’s Two-Factor Authentication (2FA) Methods.” *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 62, no. 1 (September): 1141–45. <https://doi.org/10.1177/1541931218621262>.
- Adam D. Moore, “Privacy: Its Meaning and Value”, *American Philosophical Quarterly*, 2002
- Ali. 2024. “Insider Detection Using Combination of Machine Learning and Expert Policies.” *International Journal of Electrical and Electronic Engineering & Telecommunications* 13, no. 5 (January): 389–96. <https://doi.org/10.18178/ijeetc.13.5.389-396>.
- Andrew Folks. “US State Privacy Legislation Tracker.” 2024. Iapp.org. 2024. <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>.
- Babbie, Earl R. 2020. *Practice of Social Research*. 15th ed. S.L.: Cengage Learning.
- Badri, Adarsh. 2024. “Notes: Risk Society by Ulrich Beck – Adarsh Badri.” Adarsh Badri. July 30, 2024. <https://adarshbadri.me/politics-society/notes-risk-society-by-ulrich-beck/>.
- BaMaung, David, David McIlhatton, Murdo MacDonald, and Rona Beattie. 2016. “The Enemy Within? The Connection between Insider Threat and Terrorism.” *Studies in Conflict & Terrorism* 41, no. 2 (December): 133–50. <https://doi.org/10.1080/1057610x.2016.1249776>.

- Bărbulescu v. Romania. 2017, Application no. 61496/08.
- Baxter, Jamie. 2020. Review of *Risk and Environmental Health*. In *International Encyclopedia of Human Geography*, edited by Audrey Kobayashi. Elsevier.
- Beal, Vangie. 2005. "Cyber Crime." Webopedia. January 6, 2005. <https://www.webopedia.com/definitions/cyber-crime>.
- Beck, Ulrich. "Politics of risk society." *Environmentalism. Critical Concepts* (1998): 256-266.
- Berghel, Hal. 2020. "The Equifax Hack Revisited and Repurposed." *Computer* 53, no. 5 (May): 85–90. <https://doi.org/10.1109/mc.2020.2979525>.
- Bishop, Matt. 2005. Review of *Position: "Insider" Is Relative*. In *Proceedings of the 2005 Workshop on New Security Paradigms (NSPW)*.
- Bloch, Valeska and Allens, Sophie Peach. 2018 Review of Fostering cyber awareness in a multi-vector threat environment. *"Internet Law Bulletin"*, 21(3) (52).
- Carraggi, Mike "Tewksbury Hospital Data Breach: Patients for Last 14 Years Could Be Compromised." 2017. Tewksbury, MA Patch. July 21, 2017. <https://patch.com/massachusetts/tewksbury/tewksbury-hospital-data-breach-patients-last-14-years-could-be-compromised>.
- Celcom (Malaysia) Bhd & Anor v. Tan Sri Dato' Tajudin Ramli & Ors And Another Case (No 2) [2022] 4 CLJ 381
- Chan Ah Kien v Brite-Tech Berhad & Anor [2019] MLJU 2017
- Chang, A. 2024. "Expense to Essential: The Strategic Value of Cyber Security in the Digital Age." PwC. 2024. <https://www.pwc.com/my/en/perspective/digital/Cyber-Security-strategic-value-in-digital-age.html>.
- Cheah, Donovan (BD. 2015. "Employee Privacy in Malaysia | Donovan & Ho." Donovan & Ho, Advocates & Solicitors | Malaysian Law Firm | Professional Legal Services. February 4, 2015. <https://dnh.com.my/busybodies-in-business-is-there-privacy-in-the-workplace>.
- Communications and Multimedia Act 1998
- Computer Crimes Act 1997

Cooper, Randolph B., and Robert W. Zmud. 2021. "Information Technology Implementation Research: A Technological Diffusion Approach." *Management Science* 36, no. 2 (February): 123–39.

Cyber security Act 2024.

Danny Murphy, 2024. "What Is an Insider Threat? Types, Common Indicators and Examples." Cyber Learning with Lepide. March 20, 2024. <https://www.lepide.com/blog/insider-threat-statistics-updated-for-2021>.

Dobinson, Ian, and Francis Johns. 2007. *Qualitative Legal Research; Research Methods for Law*. 2nd edn. Edinburgh University Press Ltd.

Douglas v Hello! Ltd [2005] EWCA Civ 595.

Dr Bernadine Malini Martin v MPH Magazines Sdn Bhd [2010] 7 CLJ 525

Edwards, Lilian, Laura Martin, and Tristan Henderson. 2018. "Employee Surveillance: The Road to Surveillance Is Paved with Good Intentions." *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3234382>.

Falcone, Jeremy. 2021. "The Top 10 Ways Companies Can Protect Their Confidential Information and Relationships When an Employee Joins a Competitor." Ellis & Winters LLP. Ellis & Winters LLP. November 9, 2021. <https://www.elliswinters.com/trade/the-top-10-ways-companies-can-protect-their-confidential-information-and-relationships-when-an-employee-joins-a-competitor/>.

Federal Bureau of Investigation. 2016. "Robert Hanssen | Federal Bureau of Investigation." Federal Bureau of Investigation. 2016. <https://www.fbi.gov/history/famous-cases/robert-hanssen>.

Fontes, C., & Perrone, C. (2021). Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement. *Technical University of Munich*.

Friedman, Barry A., and Lisa J. Reed. 2007. "Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-Mail Use." *Employee Responsibilities and Rights Journal* 19, no. 2 (April): 75–83. <https://doi.org/10.1007/s10672-007-9035-1>.

Fung, Carol. 2011. *Review of Collaborative Intrusion Detection Networks and Insider Attacks*. University of Waterloo.

Futó, Gilbert. 2019. "Theories of the Original Meaning of the Fourth Amendment to the United States Constitution." *Politické Vedy*, March (March), 229–46. <https://doi.org/10.24040/politickevedy.2019.22.1.229-246>.

- Genting Malaysia Bhd v Pesuruhjaya Perlindungan Data Peribadi & Ors [2022] 4 CLJ 399
- Graham Cluley, “Fired Gucci employee charged with hacking into network,” *Naked Security* by SOPHOS, April 5, 2011, <https://nakedsecurity.sophos.com/2011/04/05/fired-gucci-employee-charged-with-hacking-into-network/>
- Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. 2013. “Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations.” *The Guardian*. The Guardian. June 11, 2013. <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.
- Guido, Mark D., and Marc W. Brooks. Review of *Insider Threat Program Best Practices*. 2013. In *2013 46th Hawaii International Conference on System Sciences*. IEEE.
- Guido, Mark D., and Marc W. Brooks. Review of *Insider Threat Program Best Practices*. 2013. In *2013 46th Hawaii International Conference on System Sciences*. IEEE.
- Gunasekhar, T., K. Thirupathi Rao, and M. Trinath Basu. 2015. “Understanding Insider Attack Problem and Scope in Cloud.” *IEEE Xplore*. March 1, 2015. <https://doi.org/10.1109/ICCPCT.2015.7159380>.
- Gupta, Shibakali, and Ayan Mukherjee. 2019. “4. Use of Big Data in Hacking and Social Engineering.” *Big Data Security*, October (October), 47–74. <https://doi.org/10.1515/9783110606058-004>.
- Hadlington, Lee. 2021. “The ‘Human Factor’ in Cyber Security.” *Research Anthology on Artificial Intelligence Applications in Security*, 1960–77. <https://doi.org/10.4018/978-1-7998-7705-9.ch087>.
- Hillary, Benedict. 2023. *Nuclear Security: DOE Should Take Actions to Fully Implement Insider Threat Program : Report to the Committee on Armed Services, House of Representatives*. Edited by Daniel Will, Keya Cain, Antoinette Capaccio, Cindy Gilbert, Gwen Kirby, and Danny Royer. Washington, DC : United States Government Accountability Office.
- Insider Threat Detection Study, NATO. 2024. “Cyber Defence.” NATO. July 30, 2024. https://www.nato.int/cps/en/natohq/topics_78170.htm.
- Jaiswal, Ayshwarya, Pragya Dwivedi, and Rupesh Kumar Dewang. 2024. “Machine Learning Approaches to Detect, Prevent and Mitigate Malicious Insider

- Threats: State-of-The-Art Review.” *Multimedia Tools and Applications*, October (October). <https://doi.org/10.1007/s11042-024-20273-0>.
- Jane Ford, "The Right to Privacy in Employment: A Management Perspective" 1991.
- Jane McCallion, "Data Breaches News, Analysis and Insights | ITPro." 2024. ITPro. October 28, 2024. <https://www.itpro.co.uk/security/data-breaches/357941>.
- Jeff Hancock, "The Psychology Of Human Error – Tessian," *Tessian*, <https://www.tessian.com/research/the-psychology-of-human-error/>,
- Jones, Andy, and Carl Colwill. 2008. "Dealing with the Malicious Insider." *Australian Information Security Management Conference*, January (January). <https://doi.org/10.4225/75/57b562dab876e>.
- Jugder, Narantuya. 2016. Review of *The Thematic Analysis of Interview Data: An Approach Used to Examine the Influence of the Market on Curricular Provision in Mongolian Higher Education Institutions*. Doctoral Dissertation, The University of Leeds.
- Kandiah, Shanti. 2021. Review of *Malaysia*. In *Privacy, Data Protection and CYBER SECURITY Law Review*. The Law Review.
- Kangaie Agilan Jammany v PP [2017] 1 LNS 1640
- Kelley, P. (2023). Evolution of Cyber Attacks and Their Economic Impact. *Authorea Preprints*.
- Kure, Halima, Shareeful Islam, and Mohammad Razzaque. 2018. "An Integrated Cyber security Risk Management Approach for a Cyber-Physical System." *Applied Sciences* 8, no. 6 (May): 898. <https://doi.org/10.3390/app8060898>.
- Liu, Liu, Olivier De Vel, Qing-Long Han, Jun Zhang, and Yang Xiang. 2018. "Detecting and Preventing Cyber Insider Threats: A Survey." *IEEE Communications Surveys & Tutorials* 20, no. 2: 1397–1417. <https://doi.org/10.1109/comst.2018.2800740>.
- Liu, Liu, Olivier De Vel, Qing-Long Han, Jun Zhang, and Yang Xiang. 2018. "Detecting and Preventing Cyber Insider Threats: A Survey." *IEEE Communications Surveys & Tutorials* 20, no. 2: 1397–1417. <https://doi.org/10.1109/comst.2018.2800740>.
- MalayMail. 2022. Review of *Personal Data a Potential Gold Mine for Hackers, Malaysians Warned*, October 22, 2022. <https://www.malaymail.com/news/malaysia/2022/10/06/personal-data-a-potential-gold-mine-for-hackers-malaysians-warned/31980>.

MalayMail. 2022. Review of *Personal Data a Potential Gold Mine for Hackers, Malaysians Warned*, October 22, 2022. <https://www.malaymail.com/news/malaysia/2022/10/06/personal-data-a-potential-gold-mine-for-hackers-malaysians-warned/31980>.

Malaysia Cyber security Strategy 2020 – 2024 (2020). Prime Minister's Department: National Security Council.

Malaysian Wireless. 2023. Review of *Telekom Malaysia Reports Second Unifi Customer Data Breach within 7 Months*, July 12, 2023. <https://www.malaysianwireless.com/2023/07/personal-data-breach-unifi-telekom-malaysia/>

Maslinda Ishak v Mohd Tahir Osman [2009] 6 CLJ 653

Matt Bishop and Carrie Gates, "Defining Insider Threat", (2008), https://www.researchgate.net/publication/228993616_Defining_the_Insider_Threat (accessed November 18, 2021)

Matt Bishop and Carrie Gates, "Defining Insider Threat", (2008), https://www.researchgate.net/publication/228993616_Defining_the_Insider_Threat (accessed November 18, 2021)

Maymi, Fernando, Robert D Bixler, Randolph M Jones, and Scott D Lathrop. 2017. "Towards a Definition of Cyberspace Tactics, Techniques and Procedures." *International Conference on Big Data*, December (December). <https://doi.org/10.1109/bigdata.2017.8258514>.

Mazzarolo, Guerrino , and Anca D Jurcut. 2019. Review of *Insider Threats in Cyber Security: The Enemy within the Gates*. Doctoral Dissertation, University College Dublin.

Mazzarolo, Guerrino , and Anca D Jurcut. 2019. Review of *Insider Threats in Cyber Security: The Enemy within the Gates*. Doctoral Dissertation, University College Dublin.

Mclsaac, Barbara, Rick Shields, and Kris Klein. 2004. Review of *The Law of Privacy in Canada*. *Canadian Journal of Law and Technology*.

Merriam-Webster. 2019. "Definition of PRIVACY." Merriam-Webster.com. 2019. <https://www.merriam-webster.com/dictionary/privacy>.

Michael A. Smyth v. The Pillsbury Company (E.D. Pa. 1996), 914 F. Supp. 97

Mohamed, Ali, and Ashgar Ali. 2018. "Internet Misuse or Abuse at Workplace a Gross Misconduct," January (January).

- Mohd Fahmi Reza bin Mohd Zarin lwn Pendakwa Raya [2020] 7 MLJ 399
- Mojtaba Miri, Seyed , and Zohreh Dehdashti Shahrokh. 2019. Review of *A Short Introduction to Comparative Research*. Master's Dissertation, Allameh Tabataba'i University.
- Munir, Abu Bakar. 2012. Review of *Personal Data Protection Act: Doing Well by Doing Good*. *Malayan Law Journal*.
- Nik Adib Nik Mat v PP [2017] 1 LNS 2182
- Olabanji, Olusegun. 2019. Review of *Exploring the Application of Information Security Governance in Mitigating Insider Negligence Threats: A Qualitative Analysis*. Doctoral Dissertation, Capella University. <https://www.proquest.com/openview/3bc579b6d721814e2a6754d47ecce22f/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y>.
- Olabanji, Olusegun. 2019. Review of *Exploring the Application of Information Security Governance in Mitigating Insider Negligence Threats: A Qualitative Analysis*. Doctoral Dissertation, Capella University. <https://www.proquest.com/openview/3bc579b6d721814e2a6754d47ecce22f/1.pdf?pq-origsite=gscholar&cbl=18750&diss=y>.
- Ong Eng Guan v. Public Prosecutor [1956] 1 MLJ 44
- Panagiotis Efthymiopoulos, Marios. 2014. Review of *NATO's Cyber Defense: A Methodology for Smart Defense*. In *Cyber-Development, Cyber-Democracy and Cyber-Defense: 303 Challenges, Opportunities and Implications for Theory, Policy and Practice*.
- Personal Data Protection Act of 2010
- Peslak, Alan, and D. Scott Hunsinger. 2019. "WHAT IS CYBER SECURITY and WHAT CYBER SECURITY SKILLS ARE EMPLOYERS SEEKING?" *Issues in Information Systems* 20, no. 2: 62–72. https://doi.org/10.48009/2_iis_2019_62-72.
- Pillai, Deepak, and Yong Shih Han. n.d. Review of *The International Comparative Legal Guide to CYBER SECURITY 2019*, edited by Nigel Parker, Alexandra Rendell, Allen LLP, and Overy LLP, 130–38. Global Legal Group: r.
- Pillai, Deepak, and Yong Shih Han. n.d. Review of *The International Comparative Legal Guide to Cyber Security 2019*, edited by Nigel Parker, Alexandra Rendell, Allen LLP, and Overy LLP, 130–38. Global Legal Group: r.
- Pinto , Alex , and Gabe Bassett. 2021. Review of *2021 Data Breach Investigation Report*. Verizon.

<https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf>.

PP v Amar Asyraf Zolkepli [2021] 1 CLJ 843

PP v Roslan and Anor [2016] 1 LNS 651

PP v Vishnu Devarajan [2016] 1 LNS 1066

Pratik Chattopadhyay , Lipo Wang , and Yap-Peng Tan, “Scenario-Based Insider Threat Detection From Cyber Activities”, IEEE Transactions On Computational Social Systems, Vol. 5, No. 3, (September 2018), https://www.researchgate.net/publication/327194848_Scenario-Based_Insider_Threat_Detection_From_Cyber_Activities (accessed November 21, 2021)

Pratik Chattopadhyay , Lipo Wang , and Yap-Peng Tan, “Scenario-Based Insider Threat Detection From Cyber Activities”, IEEE Transactions On Computational Social Systems, Vol. 5, No. 3, (September 2018), https://www.researchgate.net/publication/327194848_Scenario-Based_Insider_Threat_Detection_From_Cyber_Activities (accessed November 21, 2021)

Proposal Paper [No. 5/2014] “Guide On The Management Of Cctv Under Personal Data Protection Act (PDPA) 2010

Proposal Paper [No. 5/2014] “Guide On The Management Of Cctv Under Personal Data Protection Act (PDPA) 2010

Public Bank Berhad v Tan Teck Seng Jason & Anor [2021] 1 LNS 97

Radhi, Nor Ain Mohamed. 2022. “Website Containing Malaysians’ Personal Data Taken down | New Straits Times.” NST Online. June 14, 2022. <https://www.nst.com.my/news/nation/2022/06/804941/website-containing-malaysians-personal-data-taken-down>.

Ren, Raphael, Tiong Guan Saw, and Sujata Balan. 2022. “Is There A Private Right To Privacy In Malaysia?” *IIUM Law Journal* 30, no. 1 (July): 1–32. <https://doi.org/10.31436/iiumlj.v30i1.648>.

Ren, Raphael, Tiong Guan Saw, and Sujata Balan. 2022. “Is There A Private Right To Privacy In Malaysia?” *IIUM Law Journal* 30, no. 1 (July): 1–32. <https://doi.org/10.31436/iiumlj.v30i1.648>.

Review of *Technical Code: Information and Network Security - Cyber Insurance Acquisition*. Official Website of Malaysian Communications & Multimedia Commission (MCMC).

- Richards, H. M., and L. J. Schwartz. 2002. "Ethics of Qualitative Research: Are There Special Issues for Health Services Research?" *Family Practice* 19, no. 2 (April): 135–39. <https://doi.org/10.1093/fampra/19.2.135>.
- Roslan Mohamad Som & Anor v Pendakwa Raya [2016] 1 LNS 651
- Ross, Andrew. 1990. "Hacking Away at the Counterculture." *Postmodern Culture* 1, no. 1. <https://doi.org/10.1353/pmc.1990.0011>.
- S.N. Isnin and M. Sedek. 2018. Review of *A Review on Insider Threat Status in Malaysian Organisation*. *International Journal of Academic Research in Business and Social Sciences*.
- Saxena, Neetesh, Emma Hayes, Elisa Bertino, Patrick Ojo, Kim-Kwang Raymond Choo, and Pete Burnap. 2020. "Impact and Key Challenges of Insider Threats on Organisations and Critical Businesses." *Electronics* 9, no. 9 (September): 1460. <https://doi.org/10.3390/electronics9091460>.
- Schmidt Scientific Sdn Bhd v Ong Han Suan, [1997] 5 MLJ 632
- September 22, Tracy Kitten•, and 2015. n.d. "Guilty Plea in Morgan Stanley Insider Breach." [Www.bankinfosecurity.com. https://www.bankinfosecurity.com/insider-a-8546](https://www.bankinfosecurity.com/insider-a-8546).
- Shimeall, Timothy, and Jonathan M Spring. "Introduction to Information Security: A Strategic-Based Approach." 2014. *Choice Reviews Online* 51, no. 12 (July): 51–679951–6799. <https://doi.org/10.5860/choice.51-6799>.
- Shimeall, Timothy, and Jonathan M Spring. 2014. *Introduction to Information Security : A Strategic-Based Approach*. Amsterdam ; Boston: Syngress, An Imprint Of Elsevier.
- Sivarasa Rasiah v Badan Peguam Malaysia & Anor [2010] 2 MLJ 333
- Sivarasa Rasiah v Badan Peguam Malaysia & Anor [2010] 2 MLJ 333
- Sivarasa Rasiah v Badan Peguam Malaysia & Anor [2010] 2 MLJ 333
- Sivarasa Rasiah v Badan Peguam Malaysia & Anor [2010] 2 MLJ 333
- Solms, Rossouw von, and Johan van Niekerk. 2013. "From Information Security to Cyber Security." *Computers & Security* 38, no. 38 (October): 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>.
- Spooner, Derrick, George Silowash, Daniel Costa, and Michael Albrethsen. 2018. "Navigating the Insider Threat Tool Landscape: Low Cost Technical

- Solutions to Jump Start an Insider Threat Program.” IEEE Xplore. May 1, 2018. <https://doi.org/10.1109/SPW.2018.00040>.
- Stephen M. Byars and Kurt Stanberry, *Business Ethics*. 2018. Openstax, <https://openstax.org/books/business-ethics/pages/6-4-privacy-in-the-workplace>.
- Sukhai, Nataliya B. Review of "Hacking and cybercrime. 2004." In *Proceedings of the 1st annual conference on Information security curriculum development*.
- Syahwahid, Farah, and Suriakom Miskam. 2014. Review of *Personal Data Protection Act 2010: Taking the First Steps towards Compliance* . In *Conference on Management and Muamalah*,
- Tan, Alice. 2024. "Enhancing Cyber Defense Mechanisms: AI and Machine Learning-Based Threat Mitigation Strategies." *Journal of Quantum Science and Technology* : 90-93.
- Teoh Kah Yong v. Public Prosecutor [2022] 1 LNS 2982
- The Star*. 2023. Review of *UiTM Apologises for Data Leak Involving 12,000 Varsity Applicants*, May 10, 2023. <https://www.thestar.com.my/news/nation/2023/05/10/uitm-apologises-for-data-leak-involving-12000-varsity-applicants..>
- The Star*. 2024. Review of *Cyber security Bill Tabled for First Reading*, March 30, 2024. <https://www.thestar.com.my/news/nation/2024/03/25/cyber-security-bill-tabled-for-first-reading>.
- The Star*. 2024. Review of *Cyber security Bill Tabled for First Reading*, March 30, 2024. <https://www.thestar.com.my/news/nation/2024/03/25/cyber-security-bill-tabled-for-first-reading>.
- Thompson, Shawn and Mayank Choudary. *The Ultimate Guide to Building an Insider Threat Program*. ObserveIT. (Orig. pub. 2019.).
- Toh See Wei v Teddric Jon Mohr & Anor [2017] 11 MLJ 67
- Ultra Dimension v Kook Wei Kuan [2004] 5 CLJ 285
- Umpleby, Stuart A. 2008. “A Short History of Cybernetics in the United States: The Origin of Cybernetics.” *Österreichische Zeitschrift Für Geschichtswissenschaften* 19, no. 4: 28–40. <https://doi.org/10.25365/oezg-2008-19-4-3>.
- Yiswaree Palansamy. 2022. “Minister Says Amendments to PDPA in the Works after Repeated Data Breach.” *Malay Mail* . Malay Mail. August 4, 2022.

<https://www.malaymail.com/news/malaysia/2022/08/04/minister-says-amendments-to-pdpa-in-the-works-after-repeated-data-breach/20982>.

Yusof, Ayisy . 2021. Review of *Malaysia Airlines in Data Security "Incident"*. *Business Times*, March 21, 2021.
<https://www.nst.com.my/business/2021/03/670856/malaysia-airlines-data-security-incident>



Appendix

Interview Questions used in the Study

THE APPLICATION OF MALAYSIAN CYBER SECURITY LAWS IN REGULATING CYBER INSIDER THREATS IN MALAYSIAN ORGANISATIONS INTERVIEW QUESTIONS (COURT OFFICER / JUDGE)

No	Research Question	Interview Question
1.	What are the existing laws on Malaysian CYBER SECURITY relating to the cyber insider threats management?	<ol style="list-style-type: none"> 1. How does Communications and Multimedia Act of 1998 apply to regulate cyber insider threat? 2. What are the provisions in Communications and Multimedia Act of 1998 that are applicable to cyber insider threat matters? 3. Do you think s. 233 and s. 236 of Communications and Multimedia Act of 1998 are adequate to govern cyber insider threat cases? 4. How does Computer Crimes Act 1997 apply to regulate cyber insider threat? 5. What are the provisions of Computer Crimes Act 1997 that are applicable to cyber insider threat matters? 6. Do you think s. 3 and s. 4 of Communications and Multimedia Act of 1998 are adequate to govern cyber

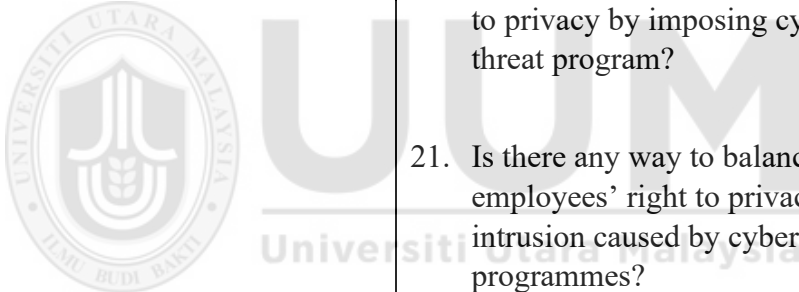
		<p>insider threat cases?</p> <p>7. How does PDPA apply to regulate cyber insider threat?</p> <p>8. What are the provisions PDPA that are applicable to cyber insider threat matters?</p> <p>9. Do you think the Security Principles of PDPA 2010 are adequate to govern cyber insider threat cases?</p> <p>10. Do you think the amendment to Sedition Act 1948 to cover electronic publications is applicable to cyber insider threat?</p>
2.	How does Malaysian CYBER SECURITY laws regulate cyber insider threats in Malaysian organisations?	<p>11. Has there been cases filed in relation to cyber incidents caused by insiders in the period your service?</p> <p>12. What is the common type of cyber insider threat that occurs in those cases?</p> <p>13. What are the common prayers prayed / damages claimed by the Plaintiff in such cases caused by cyber insider threats?</p> <p>14. What are the common provisions relied by the Plaintiff?</p> <p>15. What are the common defences pleaded by the Accused / Defendant?</p> <p>16. What are the common provisions relied</p>

		by the Defendant?
3.	What is the balancing strategy between employees' right to privacy and the intrusion caused by cyber insider threat programmes?	<p>17. Do you think cyber insider threat program is a good mechanism to prevent cyber insider incidents?</p> <p>18. Do you think the application of cyber insider threat program is intrusive to employees?</p> <p>19. Do you think employees have a right to privacy?</p> <p>20. Do you think organisations should be allowed to intrude the employees' right to privacy by imposing cyber insider threat program?</p> <p>21. Is there any way to balance the employees' right to privacy and the intrusion caused by cyber insider threat programmes?</p>

**THE APPLICATION OF MALAYSIAN CYBER SECURITY LAWS IN
REGULATING CYBER INSIDER THREATS IN MALAYSIAN
ORGANISATIONS
INTERVIEW QUESTIONS (LEGAL PRACTITIONERS)**

No	Research Question	Interview Question
1.	What are the existing laws on Malaysian CYBER SECURITY relating to the cyber insider threats management?	<ol style="list-style-type: none"> 1. How does Communications and Multimedia Act of 1998 apply to regulate cyber insider threat? 2. What are the provisions in Communications and Multimedia Act of 1998 that are applicable to cyber insider threat matters? 3. Do you think s. 233 and s. 236 of Communications and Multimedia Act of 1998 are adequate to govern cyber insider threat cases? 4. How does Computer Crimes Act 1997 apply to regulate cyber insider threat? 5. What are the provisions of Computer Crimes Act 1997 that are applicable to cyber insider threat matters? 6. Do you think s. 3 and s. 4 of Communications and Multimedia Act of 1998 are adequate to govern cyber insider threat cases? 7. How does PDPA apply to regulate cyber insider threat?

		<p>8. What are the provisions PDPA that are applicable to cyber insider threat matters?</p> <p>9. Do you think The Security Principles of PDPA 2010 are adequate to govern cyber insider threat cases?</p> <p>10. Do you think the amendment to Sedition Act 1948 to cover electronic publications is applicable to cyber insider threat?</p>
2.	How does Malaysian CYBER SECURITY laws regulate cyber insider threats in Malaysian organisations?	<p>11. Has there been cases filed in relation to cyber incidents caused by insiders in the period your service?</p> <p>12. What is the common type of cyber insider threat that occurs in those cases?</p> <p>13. What are the common prayers prayed / damages claimed by the Plaintiff in such cases caused by cyber insider threats?</p> <p>14. What are the common provisions relied by the Plaintiff?</p> <p>15. What are the common defences pleaded by the Accused / Defendant?</p> <p>16. What are the common provisions relied by the Defendant?</p>

3.	<p>What is the balancing strategy between employees' right to privacy and the intrusion caused by cyber insider threat programmes?</p> 	<p>17. Do you think cyber insider threat program is a good mechanism to prevent cyber insider incidents?</p> <p>18. Do you think the application of cyber insider threat program is intrusive to employees?</p> <p>19. Do you think employees have a right to privacy?</p> <p>20. Do you think organisations should be allowed to intrude the employees' right to privacy by imposing cyber insider threat program?</p> <p>21. Is there any way to balance the employees' right to privacy and the intrusion caused by cyber insider threat programmes?</p>
----	--	---

**THE APPLICATION OF MALAYSIAN CYBER SECURITY LAWS IN
REGULATING CYBER INSIDER THREATS IN MALAYSIAN
ORGANISATIONS
INTERVIEW QUESTIONS (REGULATOR)**

No	Research Question	Interview Question
1.	What are the existing laws on Malaysian CYBER SECURITY relating to the cyber insider threats management?	<ol style="list-style-type: none"> 1. How does Communications and Multimedia Act of 1998 apply to regulate cyber insider threat? 2. How does Computer Crimes Act 1997 apply to regulate cyber insider threat? 3. How does PDPA apply to regulate cyber insider threat? 4. What are the provisions PDPA that are applicable to cyber insider threat matters? 5. Do you think The Security Principles of PDPA 2010 are adequate to govern cyber insider threat cases? 6. Do you think the amendment to Sedition Act 1948 to cover electronic publications is applicable to cyber insider threat?

2.	How does Malaysian CYBER SECURITY laws regulate cyber insider threats in Malaysian organisations?	<p>7. Has there been cases reported in relation to cyber incidents caused by insiders in the period your service?</p> <p>8. What is the common type of cyber insider threat that occurs in those cases?</p> <p>9. Such cases will be investigated under which legal provisions?</p> <p>10. What are the common provisions relied by regulators in investigating cases caused by cyber insider threat?</p> <p>11. Do you think the current existing cyber security provisions are adequate to cater to the rising of incidents related to cyber insider threats?</p>
3.	What is the balancing strategy between employees' right to privacy and the intrusion caused by cyber insider threat programmes?	<p>12. Do you think cyber insider threat program is a good mechanism to prevent cyber insider incidents?</p> <p>13. Do you think the application of cyber insider threat program is intrusive to employees?</p> <p>14. Do you think employees have a right to privacy?</p> <p>15. Do you think organisations should be allowed to intrude the employees' right to privacy by imposing cyber insider threat program?</p> <p>16. Is there any way to balance the employees' right to privacy and the</p>

		intrusion caused by cyber insider threat programmes?
--	--	--



UUM
Universiti Utara Malaysia

**THE APPLICATION OF MALAYSIAN CYBER SECURITY LAWS IN
REGULATING CYBER INSIDER THREATS IN MALAYSIAN
ORGANISATIONS
INTERVIEW QUESTIONS (NGOs)**

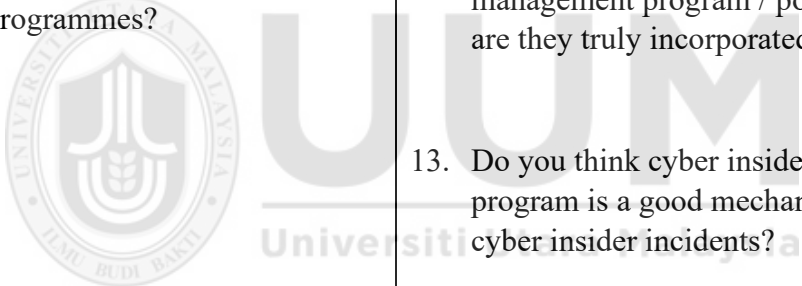
No	Research Question	Interview Question
1.	What are the existing laws on Malaysian CYBER SECURITY relating to the cyber insider threats management?	<ol style="list-style-type: none"> 1. How does Communications and Multimedia Act of 1998 apply to regulate cyber insider threat? 2. What are the provisions in Communications and Multimedia Act of 1998 that are applicable to cyber insider threat matters? 3. Do you think s. 233 and s. 236 of Communications and Multimedia Act of 1998 are adequate to govern cyber insider threat cases? 4. How does Computer Crimes Act 1997 apply to regulate cyber insider threat? 5. What are the provisions of Computer Crimes Act 1997 that are applicable to cyber insider threat matters? 6. Do you think s. 3 and s. 4 of Computer Crimes Act 1997 are adequate to govern cyber insider threat cases? 7. How does PDPA apply to regulate cyber insider threat?

		<p>8. What are the provisions PDPA that are applicable to cyber insider threat matters?</p> <p>9. Do you think The Security Principles of PDPA 2010 are adequate to govern cyber insider threat cases?</p> <p>10. Do you think the amendment to Sedition Act 1948 to cover electronic publications is applicable to cyber insider threat?</p>
2.	How does Malaysian CYBER SECURITY laws regulate cyber insider threats in Malaysian organisations?	<p>11. Has there been cases reported in relation to cyber incidents caused by insiders?</p> <p>12. What is the common type of cyber insider threat that occurs in those cases?</p> <p>13. Do you think the current existing cyber security provisions are adequate to cater to the rising of incidents related to cyber insiders?</p> <p>14. What are the examples of necessary provisions needed to regulate cyber insider threats in Malaysian organisations?</p>

3.	<p>What is the balancing strategy between employees' right to privacy and the intrusion caused by cyber insider threat programmes?</p>	<p>15. Do you think cyber insider threat program is a good mechanism to prevent cyber insider incidents?</p> <p>16. Do you think the application of cyber insider threat program is intrusive to employees?</p> <p>17. Do you think employees have a right to privacy?</p> <p>18. Do you think organisations should be allowed to intrude the employees' right to privacy by imposing cyber insider threat program?</p> <p>19. Is there any way to balance the employees' right to privacy and the intrusion caused by cyber insider threat programmes?</p>
----	--	---

**THE APPLICATION OF MALAYSIAN CYBER SECURITY LAWS IN
REGULATING CYBER INSIDER THREATS IN MALAYSIAN
ORGANISATIONS
INTERVIEW QUESTIONS (MALAYSIAN ORGANISATIONS)**

No	Research Question	Interview Question
1.	What are the existing laws on Malaysian CYBER SECURITY relating to the cyber insider threats management?	<ol style="list-style-type: none"> 1. How does Communications and Multimedia Act of 1998 apply to regulate cyber insider threat? 2. How does Computer Crimes Act 1997 apply to regulate cyber insider threat? 3. How does PDPA apply to regulate cyber insider threat? 4. What are the provisions PDPA that are applicable to cyber insider threat matters? 5. Do you think The Security Principles of PDPA 2010 are adequate to govern cyber insider threat cases? 6. Do you think the amendment to Sedition Act 1948 to cover electronic publications is applicable to cyber insider threat?
2.	How does Malaysian CYBER SECURITY laws regulate cyber insider threats in Malaysian organisations?	<ol style="list-style-type: none"> 7. Has there been cases reported in relation to cyber incidents caused by insiders? 8. What is the common type of cyber insider threat that occurs in those cases? 9. Based on the existing cyber security laws

		<p>in Malaysia, how does your organisation respond to cyber insider threat incidents?</p> <p>10. Do you think the existing cyber security laws in Malaysia is capable of regulating cyber insider threats in your organisation?</p>
3.	<p>What is the balancing strategy between employees' right to privacy and the intrusion caused by cyber insider threat programmes?</p> 	<p>11. Are there any cyber insider threat management program / policies in place?</p> <p>12. If there are such cyber insider threat management program / policies in place, are they truly incorporated?</p> <p>13. Do you think cyber insider threat program is a good mechanism to prevent cyber insider incidents?</p> <p>14. Do you think the application of cyber insider threat program is intrusive to employees?</p> <p>15. Do you think employees have a right to privacy?</p> <p>16. Do you think organisations should be allowed to intrude the employees' right to privacy by imposing cyber insider threat program?</p> <p>17. Is there any way to balance the employees' right to privacy and the intrusion caused by cyber insider threat</p>

		programmes?
--	--	-------------



**THE APPLICATION OF MALAYSIAN CYBER SECURITY LAWS IN
REGULATING CYBER INSIDER THREATS IN MALAYSIAN
ORGANISATIONS
INTERVIEW QUESTIONS (BANK OFFICER)**

No	Research Question	Interview Question
1.	What are the existing laws on Malaysian CYBER SECURITY relating to the cyber insider threats management?	<ol style="list-style-type: none"> 1. How does Communications and Multimedia Act of 1998 apply to regulate cyber insider threat? 2. How does Computer Crimes Act 1997 apply to regulate cyber insider threat? 3. How does PDPA apply to regulate cyber insider threat? 4. What are the provisions PDPA that are applicable to cyber insider threat matters? 5. Do you think The Security Principles of PDPA 2010 are adequate to govern cyber insider threat cases? 6. Do you think the amendment to Sedition Act 1948 to cover electronic publications is applicable to cyber insider threat?

2.	How does Malaysian CYBER SECURITY laws regulate cyber insider threats in Malaysian organisations?	<p>7. Has there been cases reported in relation to cyber incidents caused by insiders in Bank Negara Malaysia?</p> <p>8. What is the common type of cyber insider threat that occurs in those cases?</p> <p>9. Based on the existing cyber security laws in Malaysia, how does Bank Negara Malaysia respond to cyber insider threat incidents?</p> <p>10. Do you think the existing cyber security laws in Malaysia is capable of regulating cyber insider threats in Bank Negara Malaysia?</p>
3.	What is the balancing strategy between employees' right to privacy and the intrusion caused by cyber insider threat programmes?	<p>11. Are there any cyber insider threat management program / policies in place?</p> <p>12. If there are such cyber insider threat management program / policies in place, are they truly incorporated?</p> <p>13. Do you think cyber insider threat program is a good mechanism to prevent cyber insider incidents?</p> <p>14. Do you think the application of cyber insider threat program is intrusive to employees?</p> <p>15. Do you think employees have a right to privacy?</p>

		<p>16. Do you think organisations should be allowed to intrude the employees' right to privacy by imposing cyber insider threat program?</p> <p>17. Is there any way to balance the employees' right to privacy and the intrusion caused by cyber insider threat programmes?</p>
--	--	--



UUM
Universiti Utara Malaysia

**THE APPLICATION OF MALAYSIAN CYBER SECURITY LAWS IN
REGULATING CYBER INSIDER THREATS IN MALAYSIAN
ORGANISATIONS
INTERVIEW QUESTIONS (ACADEMICIANS)**

No	Research Question	Interview Question
1.	What are the existing laws on Malaysian CYBER SECURITY relating to the cyber insider threats management?	<ol style="list-style-type: none"> 1. How does Communications and Multimedia Act of 1998 apply to regulate cyber insider threat? 2. How does Computer Crimes Act 1997 apply to regulate cyber insider threat? 3. How does PDPA apply to regulate cyber insider threat? 4. What are the provisions PDPA that are applicable to cyber insider threat matters? 5. Do you think The Security Principles of PDPA 2010 are adequate to govern cyber insider threat cases? 6. Do you think the amendment to Sedition Act 1948 to cover electronic publications is applicable to cyber insider threat?

2.	How does Malaysian CYBER SECURITY laws regulate cyber insider threats in Malaysian organisations?	<p>7. Has there been cases reported in relation to cyber incidents caused by insiders?</p> <p>8. What is the common type of cyber insider threat that occurs in those cases?</p> <p>9. Based on the existing cyber security laws in Malaysia, how does your organisation respond to cyber insider threat incidents?</p> <p>10. Do you think the existing cyber security laws in Malaysia is capable of regulating cyber insider threats in your organisation?</p>
3.	What is the balancing strategy between employees' right to privacy and the intrusion caused by cyber insider threat programmes?	<p>11. Are there any cyber insider threat management program / policies in place?</p> <p>12. If there are such cyber insider threat management program / policies in place, are they truly incorporated?</p> <p>13. Do you think cyber insider threat program is a good mechanism to prevent cyber insider incidents?</p> <p>14. Do you think the application of cyber insider threat program is intrusive to employees?</p> <p>15. Do you think employees have a right to privacy?</p> <p>16. Do you think organisations should be</p>

		<p>allowed to intrude the employees' right to privacy by imposing cyber insider threat program?</p> <p>17. Is there any way to balance the employees' right to privacy and the intrusion caused by cyber insider threat programmes?</p>
--	--	---



LIST OF INTERVIEWEES

No	Respondent	Date of Interview	Location of Interview
1.	Judge 1	16.12.2023	Restoran Santapan Balak, Jitra
2.	Judge 2	16.12.2023	Restoran Santapan Balak, Jitra
3.	Advocate & Solicitor 1	14.10.2023	Coffee Bean & Tea Leaf, Nu Sentral
4.	Advocate & Solicitor 2	8.12.2023	Bilik Peguam, Mahkamah Tinggi Shah Alam
5.	Academician 1	16.12.2023	Restoran Santapan Balak, Jitra
6.	Academician 2	24.12.2023	Zoom Video
7.	IT Officer	18.10.2023	Zoom Video
8.	HR Officer	18.10.2023	Zoom Video
9.	Legal Counsel	23.12.2023	Zoom Video